Networks and Communications 2022

Q1

**a.i.** Botnet || Trojan

**a.ii.** Latency

**a.iii.** DNS

**a.iv.** Rollover

HARK GO DO DO DOIIS

**b.i.** Each packet is of max size 65,535 Bytes, 20 of which for IP header, 8 of which for UDP header so 28 Bytes for the header in total.

((10,200,000,000 x 37,500,000) / 65,535) \* 28 = 1.634 x 10 ^ 14 Bytes to 3.d.p = 163.4 TB

**b.ii.**

with an MSS of 1460B and a 20B header we can only send 1440B per segment

37.5\*8\*10^6 / 1440\*8 = 26041.66 ~ 26042 TCP segments required to send this clip through

1. Establishing connection:

a three way handshake for any TCP connection results in 3 segments being transmitted

2. requesting data: 1 segment

3. With Stop and Wait protocol, for each TCP segment we (server) send we have to wait for client to send back ACK

so for 26409 segments we receive back 26409 segments. Assume again that there were no corruptions or time outs and every TCP segment was delivered correctly

4. Connection termination: 4 segments

So in total the total number of segments we would send over the lifetime of this video is: 3 + 1 + 26042 \* 2 + 4 = 52092 segments

**c.i.** All I’m sure of is that Z=8

200.100.50.25 = 11001000.01100100.00110010.00011001

R0:

Address: 96.0.0.0 01100000.00000000.00000000.00000000

Netmask: 11110000.00000000.00000000.00000000

Address: 192.0.0.0 11000000.00000000.00000000.00000000

Netmask: 111 00000.00000000.00000000.00000000

We match the most with 192.0.0.0 hence X = R2

Address: 144.0.0.0 10010000.00000000.00000000.00000000

Netmask: 11110000.00000000.00000000.00000000

Address: 192.0.0.0 11000000.00000000.00000000.00000000

Netmask: 111111000.00000000.00000000.00000000

we match with neither, so take 0.0.0.0/0 i.e. Y = R6

Address: 200.100.32.0 11001000.01100100.00100000.00000000

Netmask: 11111111.11111111.11100000.00000000

Address: 200.100.48.0 11001000.01100100.001100 00.00000000

Netmask: 11111111.11111111.111111 00.00000000

we match the most with 200.100.48.0 so Z = R8

*Not sure but I think we also match R7 (unless I fucked up), and in the case of multiple matches we just take the list in order? Since all the other hops also technically had a tie with the catch all 0.0.0.0/0 and we ignored that because we found a match earlier in the list.*

**c.ii.** 552

Since the fragments need to be in multiple of 8 bytes we have:

69 \* 8 = 552

With the header included it is 552 + 20 = 572

When you do 4424 / 552 you get 8 remainder 8

So we have 9 packets in total. The offset of the last packet is 69\*8 = 552

MTU = 576B

So each offset will increase by 576/8 = 72

4444/576 = 7.715... so last fragment starts with 72\*7 = 504

**d.** All three are bots:

A ((100 x 10^6 x 8) / (5 x 10 ^ 8)) / 3 = 0.5333 = 53.3%

B ((4 x 10^6 x 8) / (80 x 10 ^ 6)) / 0.5 + ((4 x 10^6 x 8) / (80 x 10 ^ 6)) = 0.4444 = 44.4%

C 0.8 / 0.93 + 0.8 = 86% (as L/R = 800ms, also this calculation was a complete guess)

**e.i.** The HTTP response OK code should be 200.

The HTTP port should be 80 not 8080.

You have connected to the incorrect IP address (it was specified to be 146.169...)

It says 37.856K received missing a B in KB for kilobytes.

The bytes were received not sent on the last line (almost definitely wrong <skull emoji>).

Timeout expected before reaching 208s

path to object is not image/jpg, but just plur.jpg??

Should be http:// instead of http::// ?

1KB = 1024B conversion used in wget? (I tried wget in bash with a random picture, it shows 5.83K = 5969(B))

**e.ii.** (37856 / 208) \* 8 = 1456Kbps

37856B = 302848b

302848b/208s = 1456bps = 1.46Kbps

**e.iii.** They could sniff the packets that you receive, being able to access information such as source and destination IP address in the packet header.

But as HTTP is used and not HTTPS, they would also be able to access the data unencrypted because HTTP does not encrypt data.

Q2

**a.** ***Lol, so who’s gonna take this one?... 1Mbps cuz I googled it.***

LOOOOL

**b.i.** Alice's laptop and the REHL server. (Someone can double check) Might want to give Bob’s laptop a check too

**b.ii.** Create a backup of all critical data, but to prevent the backups also being affected by the ransomware they must be isolated from the network.

Keep operating systems updated to the latest patches.

Apply principle of least privilege to all systems to restrict users' ability to install software that could be malicious.

Use a proxy server or a virtual private network.

Have a Application-level gateway installed on all hosts

**c.** Unlike UDP, TCP establishes a connection before communicating and as part of that has an ACCEPT stage in which it blocks to wait for a client to connect. Having multiple threads would allow for the server to wait to connect with multiple users at the same time. I spoke about “If there is only one thread that serves all clients, then all the others would be put in a queue. This would increase the amount of time that later users have to wait for their request to be processed.” and “If you have multiple threads, then you can service multiple people at once which decreases the amount of wait time and can potentially serve peoplef immediately. If demand is still high and there are still people on the queue, this will be resolved quickly because there are more worker threads processing request.”

Also could be worth mentioning that ACCEPT is usually blocking

**d.i.** This is a problem because users might use it to add information that would help hackers find out the password.

**d.ii.** This means the website's server has stored your password rather than its hash which is bad because if a hacker were to hack the website's database, then they would have access to your password in plain text. Storing the hash means the information should not help the hacker as long as the hash function is irreversible.

**e.** One issue is that communication is more difficult over video call which is associated with the Application layer.

Another issue is that we use more scarce natural resources such as copper to facilitate our technology which is associated with the physical layer.

Finally, we must spend more on network devices to connect our networks such as switches associated with the data link layer.

Network load during peak hours, for example, a lecture or an exam is high; therefore the load on servers or CDNs that host either pre-recorded lectures or Servers that host online lectures could have a hard time coping with the number of requests coming in. Since requests operate on the Transport layer, this is a Layer 4 concern.

People might live in a part of the world where they ban certain types of media that isn't on a white list. If someone was to try and remotely study from one of these highly monitored, controlled countries (the classic example being North Korea) then the Gateways out of Korea would block the traffic from ever leaving the country. Hence they would never be able to obtain the materials and resources required to study. Since this is an issue with network security, this is a Layer 3 concern.